



研究与开发

一种新的基于指纹与人脸特征级融合的模糊金库方案

李洵, 游林, 梁家豪, 颜春辉

(杭州电子科技大学通信工程学院, 浙江 杭州 310018)

摘要: 针对基于生物特征的模糊金库易受相关攻击导致密钥和生物特征模板丢失以及基于单生物特征的模糊金库的认证性能不可靠的问题, 提出了一种新的基于指纹与人脸特征级融合的模糊金库方案。该方案对指纹特征与人脸特征分别进行不可逆变换, 并基于 Diffie-Hellman 算法在特征级变换后将指纹与人脸特征融合为一个模板。最后, 将所得的融合模板用来构建模糊金库, 通过更新随机矩阵使金库具备可撤销特性, 有效抵御相关攻击, 实现可靠的身份认证。实验结果表明, 本文方案提高了系统的可靠性和多生物特征模板的安全性。

关键词: 模糊金库; 指纹特征; 人脸特征; 模板保护; 身份认证

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018205

A novel fuzzy vault scheme based on the feature level fusion of fingerprint and face features

LI Xun, YOU Lin, LIANG Jiahao, YAN Chunhui

College of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, China

Abstract: Aiming at the problem that the biometric feature-based fuzzy vault is vulnerable to correlation attack and the loss of key and biometric template, and the authentication performance of fuzzy vault based on single biometric feature is unreliable, a novel fuzzy vault scheme based on the feature level fusion of fingerprint and face features was proposed. This scheme carried out irreversible transformation of fingerprint features and face features, and based on the Diffie-Hellman algorithm, the transformed fingerprints and face features were fused into a template at the feature level. Finally, the fusion template was used to construct the fuzzy vault. By updating the random matrix, the vault could be revoked, which could effectively resist the correlation attacks and achieve reliable authentication. Experimental results show that the proposed scheme improves the reliability of the system and the security of multiple biometric templates.

Key words: fuzzy vault, fingerprint feature, face feature, template protection, identity authentication

1 引言

基于生物特征的模糊金库^[1]是生物特征加

密领域最为经典的实用化方案, 它将用户的生物特征与秘密信息绑定生成真实点, 通过加入大量的杂凑点生成金库, 在保护秘密信息的同

收稿日期: 2018-01-10; 修回日期: 2018-06-27

时加密生物特征模板,利用生物特征的唯一性提供良好的认证性能,因此被广泛应用于身份认证与生物特征模板加密之中^[2-6]。然而,参考文献[7]指出相关攻击可从基于生物特征的模糊金库中获取到真实点,例如比较同一手指对应的两个金库来得到真实点,其易受相关攻击的原因在于人体的生物特征具有不变性,这也意味着一旦攻击者得到了真实点,用户的生物特征模板将永久丢失。

为了提高基于生物特征的模糊金库的安全性,将生物特征变换的方法应用于模糊金库。参考文献[8]使用 Hadamard 变换对指纹特征进行变换,通过改变真实点的位置来抵御相关攻击。参考文献[2]提出了可撤销模糊金库和周期变换的生物特征模板保护方案,其方法是在与密钥绑定之前首先使用周期函数对生物特征进行不可逆变换。参考文献[9]提出基于变换指纹特征的可撤销模糊金库算法,其策略也是先对指纹特征进行变换再与密钥绑定。然而,这些方案均是针对单一生物特征提出的。而在已有的多生物特征的模糊金库方案中,如参考文献[5]提出将指纹特征与虹膜特征在特征级融合,并使用融合信息构建模糊金库;参考文献[10]提取虹膜、视网膜、指静脉的细节点特征并在特征级融合,进而构建模糊金库;参考文献[11]提出了基于模糊金库的多生物特征识别系统;但这些方案均未考虑生物特征模板是否具备可撤销性以及相关攻击可能带来的安全隐患。另外,虽然基于多生物特征的模糊金库可提高认证的可靠性,但实现难点在于不同的生物特征具有不同的特征空间结构,引入多种生物特征有可能会造成维数灾难^[12],特别是应用于模糊金库中,真实点过多势必会降低整个系统的安全强度。

针对上述问题,本文将模糊金库与生物特征变换相结合,提出基于指纹与人脸特征级融

合的模糊金库方案。方案中基于 Diffie-Hellman 算法在特征级将指纹与人脸特征融合为一个模板,并将融合模板用于构建模糊金库,通过更新随机矩阵使金库具备可撤销性,令攻击者难以通过相关攻击获得金库中的真实点信息,从而提高系统的可靠性和生物特征模板的安全性。

2 生物特征加密技术

2.1 自动配准的指纹模糊金库

模糊金库的思想被提出后,指纹模糊金库方案首先被提出并进行实现,但早期的方法均使用了经过校准的指纹图像,这显然不符合实际。事实上,模糊金库虽具有良好的容错能力,但却仅限于生物特征的数量及顺序的变化,当面对较大类内差时,如指纹的旋转、平移及扭曲,将致使模糊金库实现困难。为解决这一难题,参考文献[13]根据几何散列技术提出了一种模糊金库中指纹特征自动配准的方案,其方法如下所述。

假设金库中的真实细节点与虚假细节点所构成的混合点集为 $F_a = \{f_a^i = (x_a^i, y_a^i, \theta_a^i, t_a^i) | i = 1, \dots, N_a\}$, 其中 f_a^i 表示第 i 个点, x_a^i 、 y_a^i 、 θ_a^i 和 t_a^i 分别表示该点的横坐标、纵坐标、方向和细节点类型,共 N_a 个点。在注册阶段,根据计算式(1)与式(2)将点 $f_a^2, f_a^3, \dots, f_a^{N_a}$ 以 f_a^1 为基准点对准且量化,其中 $f_a^j(1)$ 表示第 $j(j = 2, 3, \dots, N_a)$ 个点以 f_a^1 为基准点对准且量化后的点, $f_{tra}^j(1)$ 表示 $f_a^j(1)$ 基于 f_a^1 旋转变换后的点, α 和 β 分别为坐标量化参数和角度量化参数。随后,对 $f_a^2, f_a^3, \dots, f_a^{N_a}$ 重复与 f_a^1 相同的步骤,得到完整的注册散列表,每次变换生成一个表项,一共 N_a 个表项。验证时将用户的查询指纹细节点作为基准点生成验证散列表,将验证散列表与注册散列表进行比对,选择其中匹配数量最多的表项的基准点作为候选的真实点。



$$f_{\text{Tra}}^j(1) = \begin{pmatrix} x_{\text{Tra}}^j(1) \\ y_{\text{Tra}}^j(1) \\ \theta_{\text{Tra}}^j(1) \\ t_{\text{Tra}}^j(1) \end{pmatrix} = \begin{pmatrix} \cos(\theta_a^1) & \sin(\theta_a^1) & 0 & 0 \\ -\sin(\theta_a^1) & \cos(\theta_a^1) & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_a^j - x_a^1 \\ y_a^j - y_a^1 \\ \theta_a^j - \theta_a^1 \\ t_a^j \end{pmatrix}, 1 < j \leq N_a \quad (1)$$

$$f_a^j(1) = \begin{pmatrix} x_a^j(1) \\ y_a^j(1) \\ \theta_a^j(1) \\ t_a^j(1) \end{pmatrix} = \begin{pmatrix} \lfloor x_{\text{Tra}}^j(1) / \alpha + 0.5 \rfloor \\ \lfloor y_{\text{Tra}}^j(1) / \alpha + 0.5 \rfloor \\ \lfloor \theta_{\text{Tra}}^j(1) / \beta \rfloor \\ t_{\text{Tra}}^j(1) \end{pmatrix} \quad (2)$$

在上述框架的基础上,参考文献[14]提出根据注册指纹细节点的位置与方向信息生成杂凑点的方法来提高安全强度;参考文献[4]则结合几何散列的方法提出基于模糊金库的指纹模板保护方案;参考文献[15]通过减少注册指纹模板的信息冗余在智能卡上实现了自动对齐的指纹模糊金库。

2.2 生物特征变换

2.2.1 生物散列

生物散列(BioHashing)的基本思想是将用户的生物特征向量 $F_b \in \mathbb{R}^F$ 和该用户身份令牌中的随机矩阵 $R \in \mathbb{R}^{F' \times F}$ 进行迭代内积,即计算 $F'_b = RF_b$,得到 $F'_b = \{f_b^n | n=1, \dots, F'\}$,其中 F' 为生物特征维数, $F' \leq F$ 。随后,根据预设阈值 τ 由式(3)对 F'_b 量化得到二值序列 v_b^n ,最后通过比较二值序列来达到身份认证的目的。

$$v_b^n = \begin{cases} 0, & f_b^n \leq \tau \\ 1, & f_b^n > \tau \end{cases}, n=1, \dots, F' \quad (3)$$

上述方法由参考文献[16]首先提出,其方法是将指纹图像的小波傅里叶梅林变换特征与经过施密特正交化处理的随机矩阵做内积运算;随后,参考文献[17]又将高斯随机矩阵与人脸的PCA(principal component analysis, 主成分分析)特征做内积运算。实验表明该方法保持了良好的认证

性能,提高了生物特征模板的安全性与可撤销性。

2.2.2 生物特征不可逆变换

不可逆变换的方法是使用单向函数把生物特征从原始空间变换到另外一个空间,以变换后的模板作为认证模板,其中单向函数具有易于计算、求逆困难的特性。即便单向函数泄露,攻击者也难以恢复出原始的生物特征。由这一原理,参考文献[18]提出使用叠加的 Gaussian 核函数对指纹细节点特征进行变换。参考文献[19]提出自适应 Bloom(布隆)过滤器的框架并针对虹膜特征进行了实现。参考文献[20]基于缩减的循环卷积设计了一种免对齐的可撤销指纹模板,其不可逆特性在于攻击者无法从长度缩短的卷积输出向量中逆推出输入的原始指纹特征。

3 基于指纹与人脸特征级融合的模糊金库方案

根据 Diffie-Hellman 算法原理,两个用户可以生成一个共享密钥,由共享密钥计算出每个用户的私钥是基于有限域上离散对数问题难解性的。因此,本文将利用 Diffie-Hellman 算法把单一用户的指纹图像的特征作为该指纹图像所掌握的秘密信息,人脸图像的特征作为该人脸图像所掌握的秘密信息,将指纹特征集合和人脸特征集合通过一一交换的方式得到多个密钥,最终组成一个密钥集合,该密钥集合即指纹特征与人脸特征在特征级融合的新特征。方案中,将对指纹图像与人脸图像分别进行处理,生物特征使用的是指纹的细节点特征和人脸的 PCA 特征,并选定有限乘法群 F_p^* 及该群上的一个生成元 g 进行生物特征变换和融合,其中 p 为大素数。整个方案分为注册与验证两部分,具体步骤如下所示。

3.1 注册

注册阶段主要包括以下步骤。

步骤 1 对注册指纹图像 A 进行处理。

(1) 提取指纹细节点特征 $F_A = \{f_A^i = (x_A^i, y_A^i,$

$\theta_A^i, t_A^i | i=1, \dots, N_A\}$, 其中 f_A^i 为第 i 个指纹细节点, x_A^i, y_A^i, θ_A^i 和 t_A^i 分别表示该细节点的横坐标、纵坐标、方向和细节点类型, 一共是 N_A 个注册指纹细节点。

(2) 根据有限乘法群 $\mathbb{F}_p^*$ 和该群的生成元 g , 遍历 $i=1$ 到 N_A , 计算^[3]:

$$\begin{cases} x_{TA}^i = ((g^{x_A^i \parallel y_A^i}) \bmod p) / 256 \\ y_{TA}^i = ((g^{x_A^i \parallel y_A^i}) \bmod p) \bmod 256 \end{cases} \quad (4)$$

$$u_A^i = x_{TA}^i \parallel y_{TA}^i \quad (5)$$

其中, “ $\parallel$ ” 表示二进制串接运算, 十进制环境下的计算式为:

$$u_A^i = 256x_{TA}^i + y_{TA}^i \quad (6)$$

从而得到 $F_{TA} = \{f_{TA}^i = (x_{TA}^i, y_{TA}^i, \theta_A^i, t_A^i) | i=1, \dots, N_A\}$, $F_{UA} = \{u_A^i | i=1, \dots, N_A\}$, 指纹细节点经离散对数变换后的效果如图 1 所示。

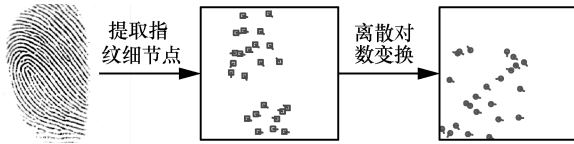


图 1 指纹细节点变换

(3) 令 F_A 中的元素作为基准点由几何散列技术^[13]生成散列表 E_A , 将 F_{TA} 中的点 f_{TA}^i 对应地替换散列表 E_A 中作为基准点的 f_A^i , 例如用 f_{TA}^1 (f_A^1 经离散对数变换得到) 替换 f_A^1 , 最后生成注册散列表 E_{TA} 。

步骤 2 对注册人脸图像 B 进行处理。

(1) 提取注册人脸的前 N_B 维 PCA 特征 $F_B = \{f_B^j | j=1, \dots, N_B\}$, f_B^j 表示第 j 维特征。

(2) 生成随机矩阵 $R \in \mathbb{R}^{N_B \times N_B}$, 其中 $R \sim N(0,1)$ 。设定阈值 τ , 对 F_B 中的 f_B^j 进行生物散列^[17], 得到 $F_{RB} = \{f_{RB}^j | j=1, \dots, N_B\}$, 其中 $f_{RB}^j \in \{0,1\}$ 。

(3) 对 F_{RB} 进行分组, 从左到右每 8 bit 为一组, 将每组转为十进制得到 $F_{IB} = \{f_{IB}^j | j=1, \dots, N'_B\}$, 其中 $N_B = 8 \cdot N'_B$ 。遍历 $j=1$ 到 N'_B , 计算:

$$f_{VB}^j = g^{f_{IB}^j} \bmod p \quad (7)$$

最后得到 $F_{VB} = \{f_{VB}^j | j=1, \dots, N'_B\}$, 人脸特征变换的方式如图 2 所示。

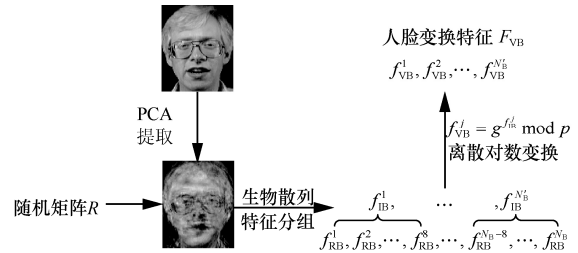


图 2 人脸特征变换

步骤 3 基于 Diffie-Hellman 算法的特征级融合

(1) 对于每个 $u_A^i \in F_{UA}$, 在 F_{VB} 中查找与 u_A^i 距离最小 (差值的绝对值最小) 的元素记为 α^i , $\alpha^i \in F_{VB}$ 。

(2) 由式 (8) 对 u_A^i 和 α^i 在特征级进行融合, 从而得到注册融合模板 $F_{AB} = \{f_{AB}^i | i=1, \dots, N_A\}$ 。

$$f_{AB}^i = ((g^{u_A^i})^{\alpha^i}) \bmod p \quad (8)$$

步骤 4 随机生成密钥 S , 并添加 16 bit 长度的 CRC (cyclic redundancy check, 循环冗余校验码) 得到 S_{CRC} , 将 S_{CRC} 分为 $d+1$ 组, 令每组作为系数构造最高次为 d 的多项式 $P(x)$:

$$P(x) = \delta_d x^d + \delta_{d-1} x^{d-1} + \dots + \delta_1 x + \delta_0 \quad (9)$$

将 $F_{AB} = \{f_{AB}^i | i=1, \dots, N_A\}$ 中的 f_{AB}^i 作为多项式输入值 x 代入多项式 $P(x)$ 中, 得到模糊金库真实点 $F_L = \{f_L^i = (f_{AB}^i, P(f_{AB}^i)) | i=1, \dots, N_A\}$ 。

步骤 5 随机生成杂凑点 $C = \{c^k = (x_C^k, y_C^k) | k=N_A+1, \dots, N_C\}$, 其中 $x_C^k \neq f_{AB}^i$, 且 $y_C^k \neq P(f_{AB}^i)$ 。 N_C 为杂凑点数量, $N_C \gg N_A$ 。最后, 合并置乱 F_L 和 C 获得模糊金库 $FV = F_L \cup C$ 。

根据上述步骤, 指纹特征与人脸特征信息已根据模糊金库算法成功加密。方案中为了保证生物特征的安全性, 除了对注册几何散列表 E_{TA} 和随机矩阵 R 进行存储, 对其余信息包括原始的生物特征信息均进行丢弃, 而所得的模糊金库可在公共信道进行传输。注册阶段的整个流程如图 3 所示。

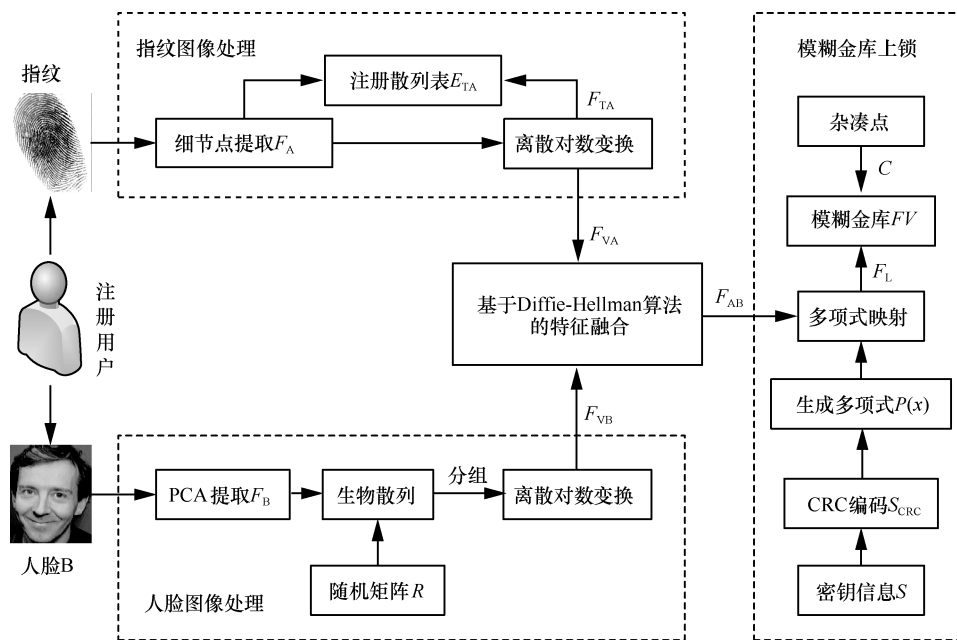


图3 注册阶段

3.2 验证

验证阶段, 流程如图4所示, 主要包括以下步骤。

步骤1 对验证指纹图像W进行处理。

(1) 提取指纹细节点特征 $F_w = \{f_w^i = (x_w^i, y_w^i, \theta_w^i, t_w^i) | i=1, \dots, N_w\}$, 其中 N_w 为验证指

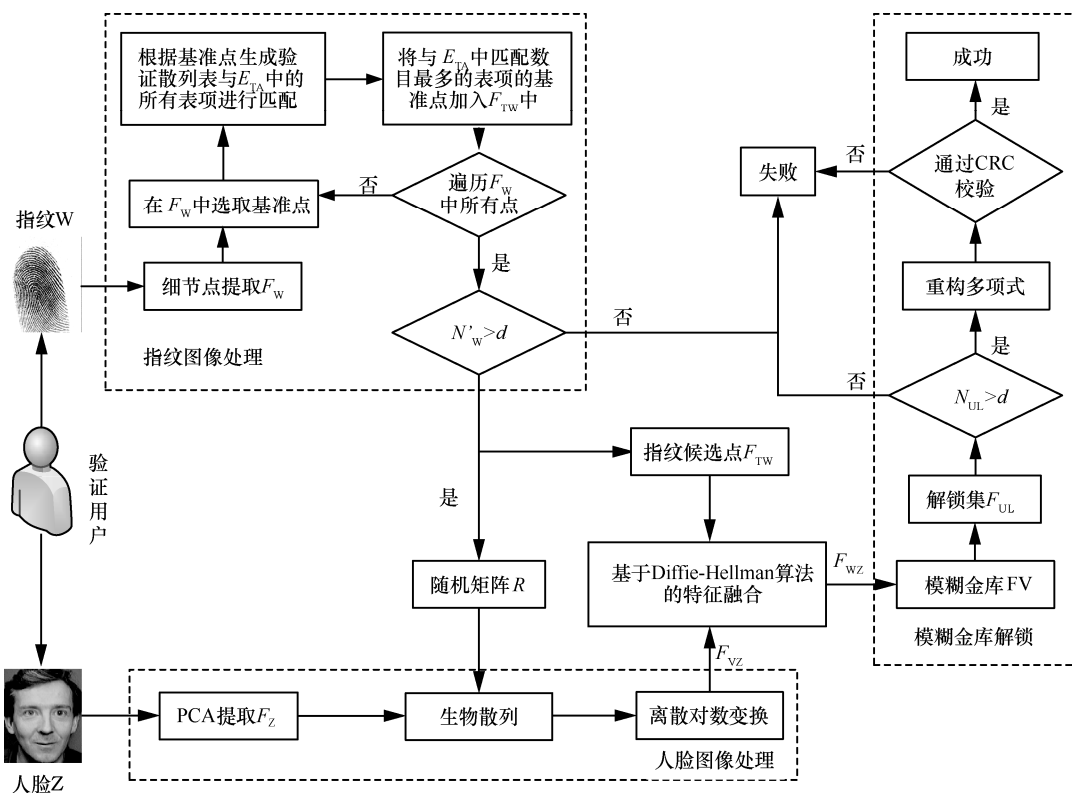


图4 验证阶段

纹细节节点的总数。以 f_w^1 为基准点由几何散列技术生成一组验证散列表，并将这组验证散列表与注册散列表 E_{TA} 中的所有表项进行匹配，将注册散列表 E_{TA} 中匹配数量最多的表项的基准点添加到指纹候选点集 F_{TW} 中。对 $f_w^2, \dots, f_w^{N'_w}$ 重复与 f_w^1 相同的步骤，获得指纹候选点集 $F_{TW} = \{f_{TW}^i = (x_{TW}^i, y_{TW}^i, \theta_{TW}^i, t_{TW}^i) | i=1, \dots, N'_w\}$ ，一共是 N'_w 个候选点。

(2) 若 $N'_w > d$ ，遍历 $i=1$ 到 N'_w ，计算：

$$u_w^i = x_{TW}^i \parallel y_{TW}^i \quad (10)$$

获得 $F_{UW} = \{u_w^i | i=1, \dots, N'_w\}$ ，并进行下一步；否则，验证失败。

步骤 2 对验证人脸图像 Z 进行处理。

(1) 提取验证人脸图像 Z 的前 N_z 维 PCA 特征 $F_z = \{f_z^j | j=1, \dots, N_z\}$ ，此处 $N_z = N_B$ 。

(2) 读取该验证用户的随机矩阵 R ，重复注册步骤 2 中的 (2)、(3)，对验证人脸特征进行不可逆变换，得到变换后的人脸特征 $F_{VZ} = \{f_{VZ}^j | j=1, \dots, N'_z\}$ ，其中 $N_z = 8N'_z$ 。

步骤 3 对 $F_{UW} = \{u_w^i | i=1, \dots, N'_w\}$ 和 $F_{VZ} = \{f_{VZ}^j | j=1, \dots, N'_z\}$ ，基于 Diffie-Hellman 算法在特征级融合，方法与注册中的步骤 3 相同，从而获得验证融合模板 $F_{WZ} = \{f_{WZ}^i | i=1, \dots, N'_w\}$ 。

步骤 4 对每个 $f_{WZ}^i \in F_{UL}$ ，查找 $y^i \in FV$ ，如点 $(f_{WZ}^i, y) \in FV$ ，则将该点添加到解锁集 F_{UL} 中，得到 $F_{UL} = \{f_{UL}^i = (x_{UL}^i, y_{UL}^i) | i=1, \dots, N_{UL}\}$ ，一共是 N_{UL} 个点，其中 x_{UL}^i 、 y_{UL}^i 分别对应 f_{WZ}^i 、 y^i 。若 $N_{UL} > d$ ，进行下一步；否则，验证失败。

步骤 5 在 F_{UL} 中任意选择 $d+1$ 个点进行组合，对其利用拉格朗日插值公式重构多项式，并使用 CRC 检验重构的多项式，若通过检验，则验证成功；否则，选择下一组组合重构多项式。若所有组合都未能通过 CRC 校验，则验证失败。

4 实验结果与分析

为了评估基于指纹与人脸特征级融合的模糊

金库的性能，本次实验选用 ORL 人脸库和 FVC2002-DB1 (DB1) 指纹库进行仿真实验。其中，ORL 人脸库中一共有 40 个样本，每个样本有 10 张图像，共 400 张图像，图像大小为 92×112 像素；DB1 指纹库中一共有 100 个指纹样本，每个样本 8 张图像，图像大小为 388×374 像素。由于 PCA 特征提取需要训练图像，故将 ORL 人脸库中的每个人脸样本的图像分为两部分，前 5 张为训练图像，后 5 张为测试图像。因此，选取 DB1 中的前 40 个样本与 ORL 结合建立指纹与人脸的多模态数据库 DB1-ORL。其中，DB1-ORL 中一共有 40 个样本，每个样本为 5 张人脸图像和 5 张指纹图像，一张人脸图像对应一张指纹图像，共 400 张图像。实验环境：惠普台式机、Windows10 系统、Visual Studio 2010 和 MATLAB r2014a。实验参数选取详情见表 1。

表 1 实验参数

参数	取值
人脸特征	$N_B = 128$ ， $\tau = 200$
CRC 校验码	CRC-16C
有限乘法群	$p = 65537$ ， $g = 3$
模糊金库运算环境	$GF(2^{16} + 1)$
杂凑点数量	$N_C = 300$

4.1 方案性能测试

在方案性能测试实验中，选用的是 GAR (genuine accept rate, 正确接受率) 和 FAR (false accept rate, 错误接受率) 作为性能评判的标准。其中，GAR 表示正确样本的生物特征成功解锁金库的百分比，FAR 表示使用错误样本的生物特征成功解锁金库的百分比。实验过程中，选取 DB1-ORL 中每个样本的第一组图像生成模糊金库，后 4 组图像用于解锁模糊金库。因此，进行 GAR 测试的总次数为 160 (40×4) 次，进行 FAR 测试的总次数为 1560 次 (40×39)。不同密钥长度下，实验结果见表 2。



表2 不同密钥长度下的 GAR 和 FAR

性能	$d = 7$	$d = 8$	$d = 9$
GAR	90.625%	90%	85.625%
FAR	0	0	0

由表2中结果可知,当多项式最高次为7~9时,本文方案的GAR分别为90.625%、90%、85.625%,随着多项式最高次的增加,GAR逐渐降低,特别是 d 由8变9时,GAR降低了4.375%,这种性能降低的原因在于人脸特征中一些有效的稳定的特征没能与指纹细节点进行结合。但是本文方案在 $d = 7$ 和8时,GAR都保持在了90%以上,并且不同密钥长度下,FAR都保持在0,表现出了很好的可靠性。

将本文方案与已有的基于单生物特征的模糊金库方案的性能对比结果见表3,表3中选取的是在 $d = 8$ 时的实验数据。根据GAR越高,FAR越低方案性能越好的准则,由表3中结果可知,在相同 d 下,本文方案使用多生物特征在DB1-ORL数据库上比参考文献[21]使用单一指纹特征在DB1数据库上的GAR高出1%,FAR低出0.04%;相比于参考文献[6]使用单一人脸特征在ORL数据库上的GAR高出5.38%,FAR低出23%;相比于在其他数据库上实现的单生物特征的模糊金库方案^[2,8],本文方案的GAR更高,且FAR=0。

由上述实验结果可知,本文方案使用多生物特征实现认证的方式比使用单一生物特征的方案性能更优。但多生物特征认证的方式使得计算量和耗时量都有所增加。 $N_c = 300$ 时,特征融合的平均耗时为119 ms,模糊金库上锁的平均耗时为

19 ms,模糊金库解锁的平均耗时为446 ms,则注册平均总耗时为138 ms,验证平均总耗时为565 ms,相比于参考文献[14]单一指纹模糊金库注册需要120 ms,验证需要469 ms,本文方案注册仅增加了18 ms,验证仅增加了96 ms。当 $d = 8$ 时,本文方案实现示例如图5所示。

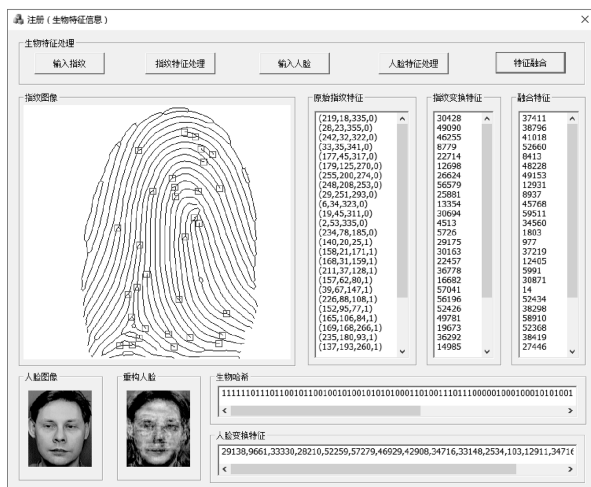
4.2 系统安全性测试

现有的针对模糊金库的相关攻击方式大多是通过比对用户多个金库中一些位置稳定不变的点来得到真实点的,但如果同一用户的多个模糊金库中的真实点位置是变化的,那么就可以有效地抵御这种攻击方式。因此,本节实验将模仿相关攻击进行系统安全性的测试。如图6是同一组图像使用相同密钥不同随机矩阵(R_1, R_2)所生成的金库及使用相关攻击的比对结果,其中,图6(a)是根据 R_1 生成的模糊金库 FV_1 ,图6(b)是根据 R_2 生成的模糊金库 FV_2 ,将这两个金库进行比对,比对效果如图6(c)所示,最终的比对结果如图6(d)所示。将得到的真实点重合量记为num,根据图6(d)的比对结果可知 $\text{num} < d$,这就使得攻击者无法通过相关攻击比对出位置固定不变的点解锁金库。

为了进一步测试本文方案中真实点的位置是可变化的,对实验进行如下设置:生成10个不同的随机矩阵,分别记为 $R_1, \dots, R_{10}$ 。将DB1-ORL中每个样本的每组指纹与人脸图像记为 T ,并将 T 分别与 $R_1, \dots, R_{10}$ 结合生成对应的真实点 $TR_1, \dots, TR_{10}$ 。之后,选取 TR_1 生成模糊金库,并将 $TR_2, \dots, TR_{10}$ 作为解锁集分别进行一次解锁操作,一共是1800(200×9)次测试。测试图像真

表3 $d=8$ 时不同方案的 GAR 和 FAR 比较

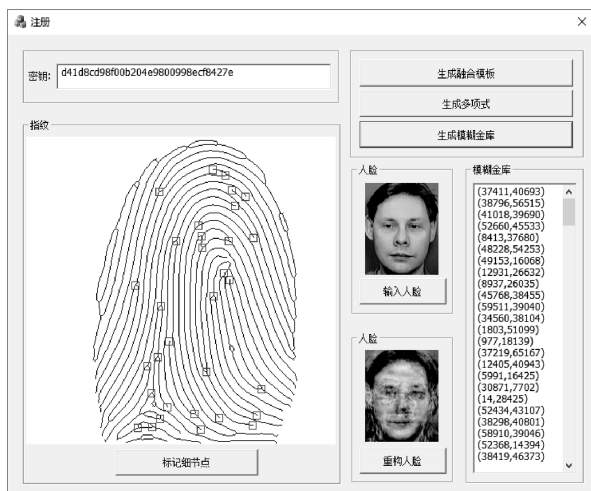
方案	数据库	生物特征	GAR	FAR
参考文献[8]方案	作者采集	指纹	89%	2%
参考文献[21]方案	DB1	指纹	89%	0.04%
参考文献[2]方案	Face94	人脸	80%	20%
参考文献[6]方案	ORL	人脸	84.62%	23%
本文方案	DB1-ORL	指纹+人脸	90%	0



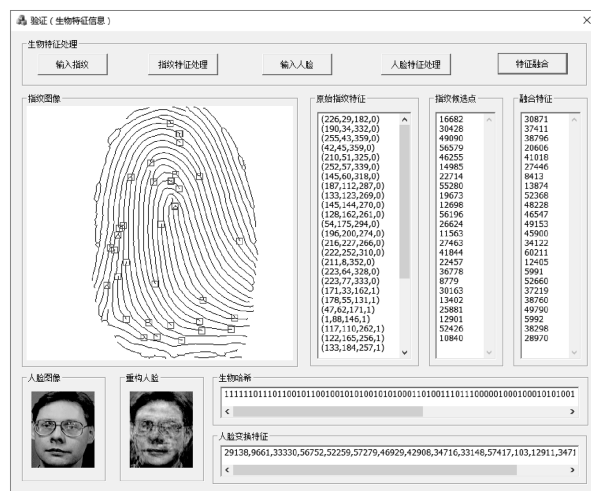
(a) 注册生物特征信息



(b) 生成公式项式



(c) 生成模糊金库



(d) 验证生物特征信息



(e) 解锁模糊金库



(f) 无效生物特征

图5 方案实现示例

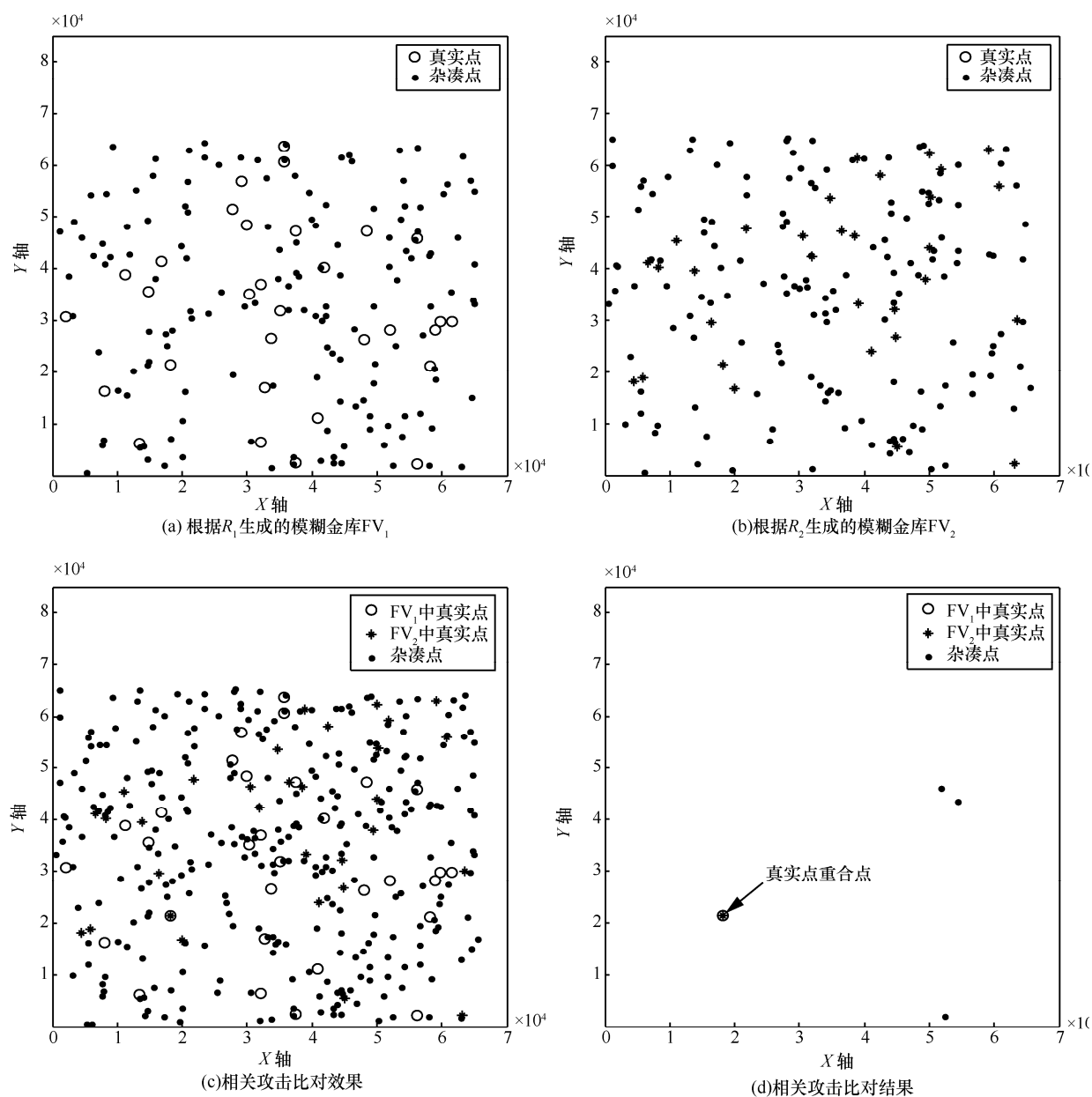


图6 同一组图像的两个模糊金库及相关攻击比对结果

实点重合量 num 的分布结果见表 4, 由表 4 中结果可知, num 的取值范围为 $0 \sim 3$, 且均未能成功解锁模糊金库 ($d = 7$)。

表4 测试图像真实点位置重合量 num 的分布结果

num	图像数量	百分比
0	1 674	93%
1	71	3.94%
2	32	1.78%
3	23	1.28%

以上真实点位置可变化的优点在于: 用户注册多个金库时, 可更新随机矩阵 R 生成不同真实点位置的金库, 防止攻击者通过相关攻击获取真实点; 另一方面, 当金库数据遭到泄露时用户可通过更新随机矩阵 R 生成一组新的真实点, 而攻击者所得到的信息将不能冒充用户通过系统的认证, 保证了身份认证的可靠性和多生物特征模板的安全。

4.3 多生物特征模糊金库性能比较

参考文献[5]指出在加密多生物特征模板时, 将

多个生物特征在特征级融合为一个模板可以提高多生物特征模板的安全性,原因在于:若攻击者得到了融合模板并试图从中获取未经处理的生物特征,则首先需要从融合模板分离出单个的生物特征。但由于不同的生物特征具有不同的特征空间结构,特征融合可能引入过高的特征维数使得匹配过程过于复杂,最终令特征级融合实现困难。

为了提高多生物特征模板的安全性实现特征级的融合,参考文献[10]提出对虹膜、视网膜和指静脉提取细节点特征,并将这 3 种生物特征的细节点混合在一起,最后使用模糊金库对这些细节点进行加密,但文中并未给出具体的实现方法。参考文献[22]通过一系列预处理对掌纹与手静脉提取共有特征点集,加入随机生成的杂凑点生成组合特征,随后将用户密钥编码成与组合特征相同的形式,并将组合特征与编码后的密钥点集混合生成金库,在验证时,通过匹配金库中所有的组合特征恢复密钥完成认证。在此基础上,参考文献[23]提出使用 DES (data encryption standard, 数据加密标准) 和 AES (advanced encryption standard, 高级加密标准) 对由掌纹、手静脉和杂凑点构成的组合特征进行双重加密,并使用加密后的特征集合构建金库。参考文献[24]提出使用 PSO (particle swarm optimization, 粒子群优化) 算法优化加入特征集合中的杂凑点位置,提取人脸与人耳共有的形状和纹理特征构建金库。但这些方案都是将多个生物特征同类型的特征直接混合,且真实点位置无法更新,若金库数据遭到泄露,多生物特征模板无法撤销,一旦攻击者破解出金库,用户的多个生物特征模板将永久丢失,从而对用户个人隐私造成不可估量的损失。为了

改进现有方案中的缺点,根据参考文献[25]指出的不同特征空间的生物特征在特征级融合时应遵循一种固定方式才能达到认证的原则,本文设计使用距离最小的方式组合指纹特征与人脸特征,从而降低特征级融合易造成维数灾难^[26]的影响。然后,基于 Diffie-Hellman 算法在特征级将指纹特征与人脸特征融合为一个模板,使融合过程不可逆,并以更新随机矩阵的方式使金库中的真实点位置可变化,解决了现有方案中的不足。

根据上述分析以及第 4.1 节中方案性能测试和第 4.2 节中系统安全性测试的实验结果,将本文方案与已实现的多生物特征的模糊金库进行比较,比对结果见表 5,其中 GAR 选取的是各方案 FAR 最低时的数据,实用性的判断标准为是否可以在现有的移动端使用,可以使用则实用性优,不可使用则实用性差。由表 5 中结果可知,虽然本文方案比参考文献[22]的 GAR 分别低了 3.375%,但本文方案的 FAR 降低了 6%,可靠性更高,且掌纹与手静脉目前还无法在移动端实现,而现有的移动设备中指纹识别与人脸识别已经可以快速准确地实现,因此本文方案的实用性更高。相比于参考文献[23-24],本文方案的 GAR 与 FAR 性能都更优。除此之外,本文方案的真实点位置是可以更新的,这提高了用户个人隐私的安全。

5 安全性分析

参考文献[2]指出理想的生物特征模板保护方案除了认证的准确性还应该具备多样性、可撤销性、不可逆的特性。本文结合生物特征变换与模糊金库算法,将经过生物散列编码和离散对数变换后的人脸特征与经过离散对数变换的指纹特征

表 5 多生物特征的模糊金库方案性能比较

方案	生物特征	GAR	FAR	真实点位置	实用性
参考文献[22]方案	掌纹+手静脉	94%	6%	不可更新	差
参考文献[23]方案	掌纹+手静脉	90%	0.1%	不可更新	差
参考文献[24]方案	人耳+人脸	90%	10%	不可更新	优
本文方案	指纹+人脸	90.625%	0	可更新	优



以距离最小的方式组合,并基于 Diffie-Hellman 算法在特征级将这两种生物特征融合为一个模板,使得存于金库中的真实点数量等于注册指纹细节点的数量。根据特征融合计算式(8)可知,改变表示人脸特征的 α^i ,表示指纹特征的 u_A^i 不变时,融合特征 f_{AB}^i 会得到更新。以上对生物特征处理方式的优点在于以下几个方面。

(1) 多样性

用户在注册多个模糊金库时,用于指纹特征的注册散列表 E_{TA} 只需注册一次,更新用于人脸特征生物散列的随机矩阵 R 可获得一组新的真实点。

(2) 可撤销性

一旦金库数据遭到泄露,也可通过(1)中方法生成新的真实点,遭到泄露的金库数据可立即作废。

(3) 不可逆性

方案中并未存储原始的生物特征,而是将经过不可逆变换的指纹特征与人脸特征基于 Diffie-Hellman 算法在特征级融合为一个模板,并将融合模板作为上锁集构建模糊金库。攻击者若要获取模板则首先需破解金库得到真实点,再通过真实点计算出用户的生物特征信息。根据攻击者所掌握的有效信息,分3种情形对方案的不可逆性进行分析与验证,具体内容如下所述。

情形一:假设攻击者得到了用户的模糊金库,试图通过暴力攻击获取其中的真实点,则攻击者需要在模糊金库中选取 $d+1$ 个点,并使用拉格朗日插值公式重构多项式。如果重构的多项式可以通过 CRC 校验,则模糊金库成功被破解;否则,攻击者需要重复上述步骤进行新一轮的尝试。根据本文方案中指纹与人脸特征的结合方式,真实点的数量是由注册指纹细节点的数量所决定的。由此,给定模糊金库 FV ,攻击者进行暴力攻击需要尝试的平均次数为:

$$\text{times} = \frac{\binom{N_A + N_C}{d+1}}{\binom{N_A}{d+1}} \quad (11)$$

当真实点数量 $N_A=30$ 、杂凑点数量 $N_C=300$ 、多项式最高次 $d=8$ 时,则金库中所有点的可能组合为 1.15×10^{17} ,其中能成功解锁金库的组合为 1.43×10^7 。因此攻击者进行暴力攻击需要尝试的平均次数 $\text{times} = (1.15 \times 10^{17}) / (1.43 \times 10^7) \approx 8.04 \times 10^9$,破解金库的概率为 $1 / \text{times} \approx 1.24 \times 10^{-10}$,如果一次解锁尝试需要 400 ms,则攻击者需要大约 101 年的时间破解金库。

情形二:假设攻击者得到了同一用户的多个模糊金库,试图通过相关攻击获取真实点,则攻击者需要对比该用户多个金库中位置固定不变的点来选出可能的真实点,并将这些可能的真实点以 $d+1$ 个为一组进行解锁尝试。而在本文方案中用户在注册多个模糊金库时使用的随机矩阵 R 是不相同的,根据本文系统安全性测试的实验结果以及融合计算式(8)可知,随机矩阵 R 的改变可令表示人脸特征的 α^i 发生改变,从而使得作为模糊金库上锁集的融合特征 f_{AB}^i 发生改变,最终令同一用户多个金库中的真实点位置具有多样性,并且不同金库中的杂凑点又是随机生成的,这就使得攻击者无法确定哪些是真实点,从而有效抵御相关攻击。

情形三:假设攻击者得到了隐藏于金库中的真实点,试图根据真实点计算出用户的生物特征信息,则攻击者需要解开融合模板,从真实点中分离出指纹特征与人脸特征,再根据分离出的信息计算出未经处理的指纹特征与人脸特征。而本文方案中对指纹特征和人脸特征均进行了基于离散对数的变换,并将变换后的指纹特征与人脸特征基于 Diffie-Hellman 算法在特征级融合为一个模板,其变换和融合的不可逆性都是基于离散对数难解问题的,攻击者想要计算出未经处理的指纹特征与人脸特征必须解决离散对数难解^[27]的问题,根据有限乘法群 F_p^* , p 为大素数,则运行的时间为 $O(p)$ 。

综上所述,本文提出的指纹与人脸特征融合的模板是满足参考文献[2]指出的各项特性的,方

案中对未经处理的原始生物特征进行了丢弃, 将经过变换的指纹特征与人脸特征基于 Diffie-Hellman 算法在特征级融合为一个模板, 其变换和融合的过程都是一个不可逆的过程, 同时以更新随机矩阵 R 的方式令同一用户的多个模糊金库的真实点位置具备多样性, 使攻击者难以通过暴力攻击和相关攻击来获取金库中的真实点。但缺点在于用户需要对随机矩阵 R 进行安全存储(可保存于辅助数据库或用户身份令牌中)来实现上述性能。

6 结束语

本文提出了基于指纹与人脸特征级融合的模糊金库方案并进行了实现, 方案中基于 Diffie-Hellman 算法在特征级将指纹与人脸特征融合为一个模板, 并使用融合模板构建模糊金库, 达到保护用户密钥和提高融合模板安全性的目的。实验结果表明, 相比于现有的单生物特征模糊金库与多生物特征模糊金库方案, 本文方案使用多生物特征实现认证, 提出的指纹与人脸特征级融合的方式, 解决了多生物特征在特征级融合易造成维数灾难和基于生物特征模糊金库易受相关攻击的问题, 提高了系统的可靠性和多生物特征模板的安全性。但是, 当多项式次数较高时, 方案的认证性能就会下降。这种性能下降的原因就在于: 提取到的指纹细节点较少, 人脸特征中一些有效的稳定的特征没能与指纹细节点进行结合。因此, 提高指纹特征提取的有效性仍然很重要, 特别是如何在存储原始指纹模板的前提下在加密域内实现指纹特征更加有效地配准是今后研究的重点。

参考文献:

- [1] JUELS A, SUDAN M. A fuzzy vault scheme [J]. *Designs Codes and Cryptography*, 2006, 38(2): 237-257.
- [2] TRAN K D, QUYNH C T, THU T B L, et al. Cancellable fuzzy vault with periodic transformation for biometric template protection [J]. *IET Biometrics*, 2016, 5(3): 229-235.
- [3] YOU L, WANG Y, CHEN Y, et al. A novel key sharing fuzzy vault scheme [J]. *KSII Transactions on Internet and Information Systems*, 2016, 10(9): 4585-4602.
- [4] MOON D, LEE S, JUNG S, et al. Fingerprint template protection using fuzzy vault[J]. *Lecture Notes in Computer Science*, 2007(4707): 1141-1151.
- [5] NANDAKUMAR K, JAIN A K. Multibiometric template security using fuzzy vault [C]//*IEEE International Conference on Biometrics: Theory, Applications and Systems*, Sept 29-Oct 1, 2008, Arlington, USA. Piscataway: IEEE Press, 2008: 1-6.
- [6] WU L, YUAN S. A face based fuzzy vault scheme for secure online authentication [C]//*Second International Symposium on Data, Privacy, and E-Commerce*, Sept 13-14, 2010, Buffalo, USA. Piscataway: IEEE Press, 2010: 45-49.
- [7] SCHEIRER W J, BOULT T E. Cracking fuzzy vaults and biometric encryption [C]//*Biometrics Symposium*, Sept 11-13, 2007, Baltimore, USA. Piscataway: IEEE Press, 2007: 1-6.
- [8] KAUR M, SOFAT S. Secure fingerprint fuzzy vault using Hadamard transformation to defy correlation attack [C] //2016 Sixth International Symposium on Embedded Computing and System Design (ISED), Dec 15-17, 2016, Patna, India. Piscataway: IEEE Press, 2016: 122-126.
- [9] YOU L, YANG L, YU W, et al. A cancelable fuzzy vault algorithm based on transformed fingerprint features [J]. *Chinese Journal of Electronics*, 2017, 26(2): 236-243.
- [10] GEETIKA, KAUR M. Multimodal based fuzzy vault using iris retina and fingervein [C]//*Fourth International Conference on Computing, Communications and Networking Technologies*, July 4-6, 2013, Tiruchengode, India. Piscataway: IEEE Press, 2013: 1-5.
- [11] RAZAQUE A, SREERAMU P S, AMSAAD F H, et al. Multi-biometric system using fuzzy vault [C]// *IEEE International Conference on Electro Information Technology*, May 19-21, 2016, Grand Forks, USA. Piscataway: IEEE Press, 2016: 122-126.
- [12] RATTANI A, KISKU D R, BICEGO M, et al. Feature level fusion of face and fingerprint biometrics [C]// *IEEE International Conference on Biometrics: Theory, Applications, and Systems*, Sept 27-29, 2007, Crystal City, USA. Piscataway: IEEE Press, 2007: 1-6.
- [13] CHUNG Y, MOON D, LEE S, et al. Automatic alignment of fingerprint features for fuzzy fingerprint vault [J]. *Lecture Notes in Computer Science*, 2005(3822): 358-369.
- [14] LEE S, CHUNG Y, MOON D, et al. A practical implementation of fuzzy fingerprint vault [J]. *KSII Transactions on Internet and Information Systems*, 2011, 5(10): 1783-1798.
- [15] MOON D, CHUNG Y, SEO C, et al. A practical implementation of fuzzy fingerprint vault for smart cards [J]. *Journal of Intelligent Manufacturing*, 2014, 25(2): 293-302.
- [16] JIN A T B, LING D N C, GOH A. Biohashing: two factor authentication featuring fingerprint data and tokenised random number [J]. *Pattern Recognition*, 2004, 37(11): 2245-2255.
- [17] TEOH A B J, GOH A, NGO D C L. Random multispace quantization as an analytic mechanism for BioHashing of biometric and random identity inputs [J]. *IEEE Transactions on Pattern Analysis & Machine Intelligence*, 2006, 28(12): 1892-1901.
- [18] RATHA N K, CHIKKERUR S, CONNELL J H, et al. Generat-



- ing cancelable fingerprint templates [J]. IEEE Transactions on Pattern Analysis & Machine Intelligence, 2007, 29(4): 561-572.
- [19] SADHYA D, SINGH S K. Providing robust security measures to Bloom filter based biometric template protection schemes [J]. Computers & Security, 2017(67): 59-72.
- [20] WANG S, HU J. Design of alignment-free cancelable fingerprint templates via curtailed circular convolution [J]. Pattern Recognition, 2014, 47(3): 1321-1329.
- [21] LI P, YANG X, CAO K, et al. An alignment-free fingerprint cryptosystem based on fuzzy vault scheme [J]. Journal of Network & Computer Applications, 2010, 33(3): 207-220.
- [22] LALITHAMANI N, SABRIGIRIRAJ M. Palm and hand vein-based fuzzy vault generation scheme for multibiometric cryptosystem[J]. Journal of Photographic Science, 2014, 63(2): 111-118.
- [23] LALITHAMANI N, SABRIGIRIRAJ M. Dual encryption algorithm to improve security in hand vein and palm vein-based biometric recognition [J]. Journal of Medical Imaging & Health Informatics, 2015, 5(3): 545-551.
- [24] AMIRTHALINGAM G, RADHAMANI G. New chaff point based fuzzy vault for multimodal biometric cryptosystem using particle swarm optimization [J]. Journal of King Saud University-Computer and Information Sciences, 2016, 28(4): 381-394.
- [25] LIM M H, VERMA S, MAI G, et al. Learning discriminability-preserving histogram representation from unordered features for multibiometric feature-fused-template Protection [J]. Pattern Recognition, 2016, 60(C): 706-719.
- [26] 章坚武, 杨佳佳, 吴震东. 一种基于指纹和声纹决策级融合识别方法 [J]. 电信科学, 2018, 34(3): 32-40.
- ZHANG J W, YANG J J, WU Z D. Method of fingerprint and voiceprint based decision level fusion recognition [J]. Telecommunications Science, 2018, 34(3): 32-40.
- [27] 王崇霞, 高美真, 刘倩, 等. 混合云联合身份认证与密钥协商协议设计 [J]. 电信科学, 2014, 30(4): 95-99.
- WANG C X, GAO M Z, LIU Q, et al. Design of united identity authentication and key agreement protocol for hybrid cloud [J]. Telecommunications Science, 2014, 30(4): 95-99.

[作者简介]



李洵 (1993-), 女, 杭州电子科技大学通信工程学院硕士生, 主要研究方向为生物特征密码技术。



游林 (1966-), 男, 杭州电子科技大学通信工程学院教授、博士生导师, 主要研究方向为计算代数、密码学、生物特征识别及其应用等。



梁家豪 (1990-), 男, 杭州电子科技大学通信工程学院硕士生, 主要研究方向为生物特征密码技术。



颜春辉 (1992-), 男, 杭州电子科技大学通信工程学院硕士生, 主要研究方向为生物特征密码技术。